

ABSTRACT TO THE DISCLOSURE

Method for checking the signature of a message, the message, signature and a certificate having, been sent by a 5 signer having a public key to a recipient having a message storage device (11). According to the invention, said method comprises the stages according to which :

• The certificate in the protected device (21) connected to said storage device (11) of the recipient and 10 checked and at least one checking result data element is sent to a display device (30) connected directly to the protected device (21),

• The result data element is checked on the display device (30),

15 • When the certificate is verified, a reduction of the message is calculated in the protected device (21) and the message is recopied onto the display device (30) during the reduction operation,

20 • The signature with the public key of the signer is decrypted in said protected device (21), and

• The decrypted signature is compared with the reduction carried out,

25 • According to the result of the comparison, a message is sent from the protected device (21) to the display device (30) indicating that the signature conforms/does not conform to the message or to the public key of the signer put forward.

Application for protecting exchanges on communication networks.

30 (Figure 1)